

Effect of Intensity Modulator Extinction on Practical Quantum Key Distribution System

Jing-Zheng Huang, Zhen-Qiang Yin*, Shuang Wang, Hong-Wei Li, Wei Chen** and Zheng-Fu Han***
 Key Laboratory of Quantum Information, University of Science and Technology of China, Hefei, 230026, China
 (Dated: June 29, 2012)

We study how the imperfection of intensity modulator effects on the security of a practical quantum key distribution system. The extinction ratio of the realistic intensity modulator is considered in our security analysis. We show that the secret key rate increases, under the practical assumption that the indeterminable noise introduced by the imperfect intensity modulator can not be controlled by the eavesdropper.

I. INTRODUCTION

Quantum key distribution(QKD) is a peculiar technology that guarantees two remote parties, Alice and Bob, to share a secret key which is prevented from eavesdropping by physical laws. Since the first QKD protocol, namely the BB4 protocol, was proposed by Bennett and Brassard in 1984[1], QKD has become the primary application of quantum information science. The unconditional security of QKD, which is the biggest advantage of this technology, have already been proven in both discrete-variable protocols([2–7]) and continuous-variable protocols[8–10]. However, some assumptions in these proofs are not removable. For instance, the single-photon detectors(SPD) are usually considered to be unresponsive to bright lights in the linear mode, but it is not true. In Ref.[11], the authors experimentally prove that the SPD click can be triggered by bright light when the SPD is working in linear mode, therefore a detector-blind-attack is proposed and used to hack the commercial QKD systems successfully. For this reason, it is very important to analyze how the imperfect devices effect on the security of a practical QKD system, and the analysis of the security in practical QKD systems attracts much attention recently[12]. For examples, the decoy state method proposed by Hwang[13] has developed as a powerful tool to analyze the imperfect single-photon source and achieve the modified secret key rate[14–16], and the effect of imperfect phase modulator has also been studied by an equivalent model in[17, 18]. However, many imperfections are still not considered before. In this paper, we analyze the finite extinction of imperfect intensity modulator(IM) in the practical QKD system. Our simulation result shows that surprisingly, the extra noise introduced by the realistic IM reduces Eve's information and increases the secret key rate.

II. PRELIMINARY

In the BB84 protocol, Alice randomly encodes $\{0, 1\}$ into the rectilinear basis $\{|H\rangle, |V\rangle\}$ or the diagonal basis $\{|+\rangle, |-\rangle\}$, where $\langle H|V\rangle = 0$ and $|\pm\rangle = \frac{1}{\sqrt{2}}(|H\rangle \pm |V\rangle)$. She can produce these states by using the scheme described in Figure.1, which is applicable to the high speed

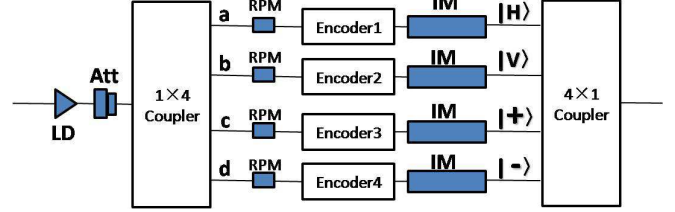


FIG. 1: The scheme diagram of producing states $|H\rangle, |V\rangle, |+\rangle$ and $|-\rangle$. LD: Laser Diode; BS: Beam Splitter; IM: Intensity Modulator; Encoder(1-4): Polarization modulator or Mach-Zehnder interferometer, corresponding to the protocol's requirement; RPM: Random Phase Modulator. The two couplers are used for splitting and recombining the laser pulses.

QKD systems[19].

In this scheme, the laser pulse generated by the laser diode is first attenuated to the single photon level, which can be written as a weak coherent state $|\mu\rangle$ ($\mu \simeq 0.2$), where μ is the amplitude of light. This state is then split by a coupler into four paths, which are described as a, b, c and d. After the random phase modulating and encoding, the coherent state becomes $|\mu\rangle \rightarrow (|e^{i\theta_a} \frac{\mu}{2}\rangle_{a,H} + |e^{i\theta_b} \frac{\mu}{2}\rangle_{b,V} + |e^{i\theta_c} \frac{\mu}{2}\rangle_{c,+} + |e^{i\theta_d} \frac{\mu}{2}\rangle_{d,-})$, where $\theta_{a,b,c,d}$ denote the additional random phases. The intensity modulators(IM) are then used to filter out the components of the state that we do not need. Depending on the electro-optic effect, we can control the attenuation of IM by supplying an appropriate voltage on it. The state of IM is denoted as "off" when it has high attenuation and "on" when it has nearly no attenuation. The amplitude of light is attenuated by a factor of $\sqrt{P_{off}}$ or $\sqrt{P_{on}}$ when the state of IM is off or on, and the power of the output light is $I_{off} = P_{off}I_0$ or $I_{on} = P_{on}I_0$ respectively, where $I_0 = |\frac{\mu}{2}|^2$ denotes the power of the input light. Then the extinction ratio of IM can be defined as[20]:

$$r := \frac{I_{on}}{I_{off}}. \quad (1)$$

For simplicity, we assume the four IM have the same extinction ratio. Without loss of generality, we suppose that Alice produces the signal state $|H\rangle$. Note that only the single photon state can take part in the secret key generation[7], we consider the single photon state directly. After the 4x1 coupler, the single photon state

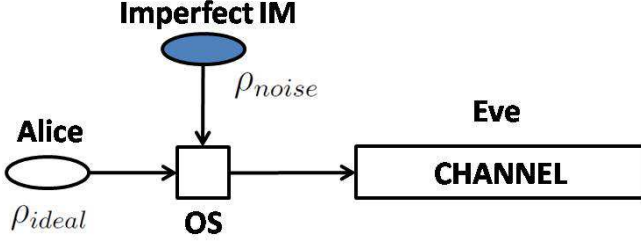


FIG. 2: The equivalent model diagram of the state generation process. OS is an optical switch that randomly routes ρ_{ideal} or ρ_{noise} to the channel with $\frac{r-1}{r+3}$ or $\frac{4}{r+3}$ probability. ρ_{ideal} , ρ_{noise} and r are defined in the text.

at the output port can be written as (see the Appendix section for more details):

$$\rho_H = e^{-\frac{(P_{on}+3P_{off})\mu^2}{8}} \left[\frac{(P_{on}+3P_{off})\mu^2}{8} \right] \times \left(\frac{r-1}{r+3} |H\rangle\langle H| + \frac{4}{r+3} \hat{I} \right). \quad (2)$$

After normalizing, the single photon part of any signal state produced by this modulation process can be generally written as:

$$\rho_{signal} = \frac{r-1}{r+3} \rho_{ideal} + \frac{4}{r+3} \rho_{noise}. \quad (3)$$

Where ρ_{ideal} denotes the pure signal state ($|H\rangle\langle H|$, $|V\rangle\langle V|$, $|+\rangle\langle +|$ or $|-\rangle\langle -|$), and $\rho_{noise} = \frac{1}{2} \hat{I}$ is the density matrix of the extra noise introduced by the finite extinction ratio of IM. Figure.2 shows the equivalent model description of the state generation process.

III. SECURITY PROOF

In this section, we prove the security of the practical QKD system using the state generation scheme described in Fig.1. We first analyze the security in the case of BB84 protocol with ideal single photon state, and then generalize our result by combining the decoy state method.

A. BB84 protocol with single photon state

The secret key rate of BB84 protocol with ideal single photon state can be written as[7]:

$$R_s = 1 - H(e_1) - H(e_1). \quad (4)$$

Where e_1 is the quantum error bit rate (QBER) caused by the noises in the channel and detectors, and $H(x) = -x \log_2 x - (1-x) \log_2 (1-x)$ is the Shannon entropy function. In the security analysis, all of the errors are considered to be introduced by Eve when she tries to achieve secret key information from the signal state. Equation (4) shows that a fraction $H(e_1)$ of the sifted key is sacrificed to perform error correction, and the same

amount of information is sacrificed to perform privacy amplification[7].

As we have analyzed in section 2, the imperfection of IM introduce extra noises, therefore the QBER should be modified as:

$$e'_1 = e_1 \cdot \frac{r-1}{r+3} + \frac{1}{2} \cdot \frac{4}{r+3} = (1 - \frac{4}{r+3})e_1 + \frac{2}{r+3}. \quad (5)$$

The second part of the right hand side of this equation is due to the 50% error rate introduced by ρ_{noise} . Note that the identity matrix remains unchanged under all unitary operations, so that Eve can not achieve any useful information by performing any operation on it. Therefore this part of errors are impossible to be introduced by Eve. For this reason, only a fraction $(1 - \frac{4}{r+3})$ of the sifted key need to perform the privacy amplification process[7]. We rewrite e_1 as a function of e'_1 from Eq.(5):

$$e_1 = \frac{e'_1 - p}{1-2p}. \quad (6)$$

Where $p \equiv \frac{2}{r+3}$. The modified secret key rate can now be written as follow:

$$R'_s = 1 - H(e'_1) - (1-2p)H(e_1) = 1 - H(e'_1) - (1-2p)H(\frac{e'_1 - p}{1-2p}). \quad (7)$$

B. BB84 protocol with decoy state method

For preventing the photon number splitting (PNS) attack, decoy state method is an essential tool in practical QKD system[14, 15]. The secret key rate of the BB84 protocol with decoy state method is given by[15]:

$$R_d = q \{ -Q_\mu f(E_\mu) H(E_\mu) + Q_1 [1 - H(e_1^U)] \}; \quad (8)$$

$$Q_\mu = \sum_{i=0}^{\infty} Y_i e^{-\mu} \frac{\mu^i}{i!}, \quad Q_\mu E_\mu = \sum_{i=0}^{\infty} Q_i e_i. \quad (9)$$

Where q is the efficiency of the protocol which equals $\frac{1}{2}$ in the BB84 protocol,

Y_i is the yield of an i -photon state,

Q_μ is the gain of the signal states,

E_μ is the average QBER,

e_i is the QBER caused by the i -photon state,

e_1^U is the upper bound of e_1 ,

$f(x)$ is the bidirectional error correction efficiency as a function of error bit rate[22]. e_1^U can be estimated by[16]:

$$e_1^U = \frac{e_0 Y_0 + e_{detect} \eta}{Y_0 + \eta}. \quad (10)$$

Where η is the detection efficiency of the QKD system, $e_0 = \frac{1}{2}$ is the error bit rate caused by the vacuum state and e_{detect} is the error bit rate caused by the system imperfection, which includes the error bit rate introduced by the imperfect IM. These two parameters can both be obtained from the field test experiments (e.g. [23]).

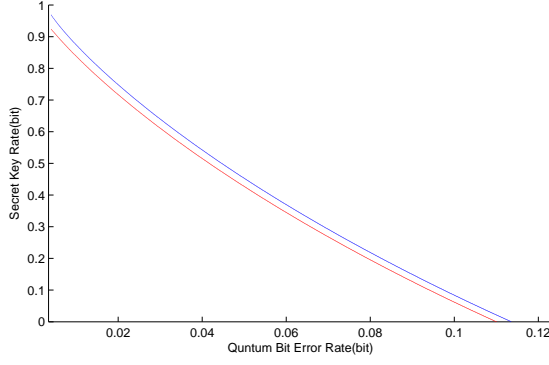


FIG. 3: The simulation result of the modified secret key rate in the case of using ideal single photon state. The modified result in our analysis which has the maximum tolerable QBER of 11.37% is described in blue line, comparing to the one using the GLLP method[7], which is described in red line. In this simulation, the extinction ratio of IM is assumed to be 27dB.

Using Eq.(6), we get the error bit rate introduced by the ideal single photon state ρ_{ideal} in Eq.(3) as:

$$\begin{aligned} e_{detect} &\rightarrow \frac{e_{detect} - p}{1 - 2p} \\ e_1^U &\rightarrow \frac{\frac{Y_0}{2} + (e_{detect} - p)\eta / (1 - 2p)}{Y_0 + \eta} \equiv e_1^d. \end{aligned} \quad (11)$$

Using the similar method in section 3.1, we achieve the modified secret key rate of BB84 protocol with the decoy state method by considering the effect of IM extinction ratio as follow:

$$R'_d = q\{-Q_\mu f(E_\mu)H(E_\mu) + Q_1(\frac{Y_0 + (1-2p)\eta}{Y_0 + \eta})H(e_1^d)\}. \quad (12)$$

IV. SIMULATIONS

Fig.3 and Fig.4 show the numerical simulations of Eq.(7) and Eq.(12) respectively. Here we assume the extinction ratio of IM to be 500(27dB), which is a reasonable value depending on the testing result of the IM in our field test experiment[23]. In Fig.3, we simulate the relation between secret key rate and QBER in BB84 protocol with ideal single photon state. We find that the maximum tolerable QBER increases to 11.37%, comparing with 11% when using the GLLP method. Because the background noises caused by the imperfect IM always exist, the QBER labeled on lateral axis does not start at zero.

In the case of BB84 protocol with the decoy state method, we simulate the relation between secret key rate and transportation distance by using the key parameters for QKD experiment in[23]. Fig.4 shows that in our analysis the maximum secure transportation distance is 120.6km, comparing to 119.9km by using the previous analysis method[16], and the secret key rates we achieved in [23] increase 3% - 4%(see table 1) in the modification.

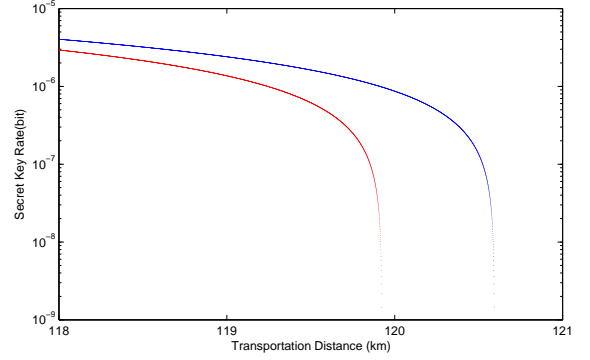


FIG. 4: The simulation result of the modified secret key rate in the case of using decoy state method. The red line describes the optimal estimation of the secret key rate using the method in[16] and experiment data in[23]. By considering the extra noise introduced by the imperfect IM, the estimation of secret key rate using the modified method in our paper which is described in blue line. In this simulation, the extinction ratio of IM is 27dB.

TABLE I: The secret key rates calculated by[23] and modified by this paper, in units of kbit/s. The items in the first row denote the different communication channels of the QKD network stated in [23].

QKD Channels	A2R2B	A2R2C	D2R2A	E2R2A
Secret key (in [23])	4.91	2.02	1.82	0.41
Secret key (in this paper)	5.09	2.09	1.88	0.43

V. CONCLUSION

The effect of the IM extinction on practical QKD system is analyzed in paper. We surprisingly found that Eve loses more information than Alice and Bob in the process of realistic intensity modulation. We improved the lower bound of secret key rate of BB84 protocol with ideal single photon state and decoy state method respectively, and compare them to the previous security analysis in numerical simulation. Our study makes an effort to consummate the security analysis of the realistic devices in practical QKD systems. Moreover, the security of the other realistic devices can also be analyzed by the approach we derived in this paper.

Acknowledgements

This work was supported by the National Basic Research Program of China (Grants No. 2011CBA00200 and No. 2011CB921200), National Natural Science Foundation of China (Grants No. 60921091 and No. 61101137), and China Postdoctoral Science Foundation (Grant No. 20100480695).

*To whom correspondence should be addressed, Email:

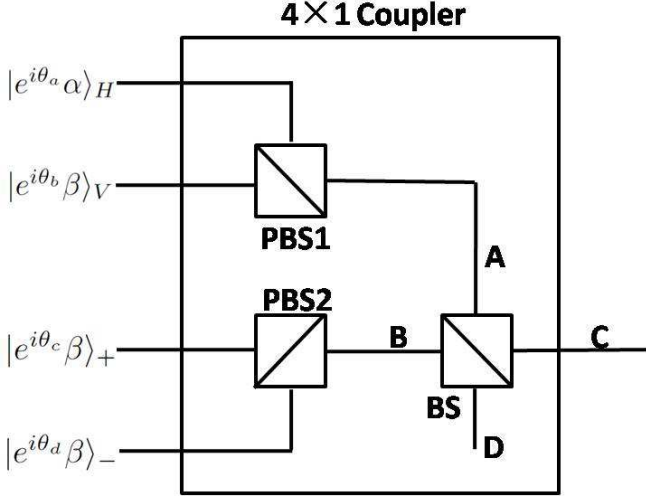


FIG. 5: The 4×1 coupler used in polarization encoding. PBS: Polarization Beam Splitter; BS: Beam Splitter. The four paths of the BS are denoted by A, B, C and D. The four input coherent states are defined in the text.

yinzheqi@mail.ustc.edu.cn.

**To whom correspondence should be addressed, Email: kooky@mail.ustc.edu.cn

***To whom correspondence should be addressed, Email: zfhfan@ustc.edu.cn

Appendix

Here we derive the expressions of Eq.(2) and Eq.(3) in section 2. We analyze the case of polarization encoding, which uses the 1×4 coupler described in Fig.5. The similar analysis can be also applied to the phase encoding case and obtains the same result.

As we have mentioned in section 2, after the random phase modulating and encoding, the four coherent states input to the 4×1 coupler are $|e^{i\theta_a}\sqrt{P_{on}}\frac{\mu}{2}\rangle$, $|e^{i\theta_b}\sqrt{P_{off}}\frac{\mu}{2}\rangle$, $|e^{i\theta_c}\sqrt{P_{off}}\frac{\mu}{2}\rangle$ and $|e^{i\theta_d}\sqrt{P_{off}}\frac{\mu}{2}\rangle$, when we assume Alice produces the H state. Let us denote $\alpha = \sqrt{P_{on}}\frac{\mu}{2}$ and $\beta = \sqrt{P_{off}}\frac{\mu}{2}$. After combining by the polarization beam splitters, we get two output coherent states written in the form of creation operators acting on vacuum states:

$$\begin{aligned}
 |e^{i\theta_a}\alpha\rangle_H |e^{i\theta_b}\beta\rangle_V &\rightarrow e^{-\frac{\alpha^2+\beta^2}{2}} \sum_{n=0}^{\infty} \frac{(e^{i\theta_a}\alpha a_H^\dagger + e^{i\theta_b}\beta a_V^\dagger)^n}{n!} |0\rangle_A \\
 &= e^{-\frac{\alpha^2+\beta^2}{2}} \sum_{n=0}^{\infty} \frac{(A^\dagger)^n}{n!} |0\rangle_A, \\
 |e^{i\theta_c}\beta\rangle_+ |e^{i\theta_d}\beta\rangle_- &\rightarrow e^{-\beta^2} \sum_{m=0}^{\infty} \frac{\beta^m (e^{i\theta_c}a_+^\dagger + e^{i\theta_d}a_-^\dagger)^m}{m!} |0\rangle_B \\
 &= e^{-\beta^2} \sum_{m=0}^{\infty} \frac{\beta^m (e^{i\theta'_c}a_H^\dagger + e^{i\theta'_d}a_V^\dagger)^m}{m!} |0\rangle_B \\
 &= e^{-\beta^2} \sum_{m=0}^{\infty} \frac{(B^\dagger)^m}{m!} |0\rangle_B.
 \end{aligned} \tag{13}$$

Where a^\dagger denotes the creation operator with the subscript of different polarizations. And we also define $e^{i\theta'_c} \equiv \frac{e^{i\theta_c} + e^{i\theta_d}}{2}$ and $e^{i\theta'_d} \equiv \frac{e^{i\theta_c} - e^{i\theta_d}}{2}$; $A^\dagger \equiv e^{i\theta_a}\alpha a_H^\dagger + e^{i\theta_b}\beta a_V^\dagger$

and $B^\dagger \equiv \beta(e^{i\theta'_c}a_H^\dagger + e^{i\theta'_d}a_V^\dagger)$ in the above expressions. The coherent states before inputting to the beam splitter can be written in direct product form as follows:

$$\begin{aligned}
 &e^{-\frac{\alpha^2+\beta^2}{2}} \sum_{n=0}^{\infty} \frac{(A^\dagger)^n}{n!} |0\rangle_A \otimes e^{-\beta^2} \sum_{m=0}^{\infty} \frac{(B^\dagger)^m}{m!} |0\rangle_B \\
 &= e^{-\frac{\alpha^2+\beta^2}{2}} \sum_{n,m=0}^{\infty} \frac{(A^\dagger)^n (B^\dagger)^m}{n!m!} |00\rangle
 \end{aligned} \tag{14}$$

At the output ports, the beam splitter transforms each term of the above operator polynomial into:

$$\begin{aligned}
 \frac{(A^\dagger)^n (B^\dagger)^m}{n!m!} &\rightarrow \left(\frac{1}{\sqrt{2}}\right)^{m+n} \frac{(C_A^\dagger + D_A^\dagger)^n (C_B^\dagger - D_B^\dagger)^m}{n!m!} \\
 &= \frac{1}{\sqrt{2}^{m+n}} \frac{1}{n!m!} \sum_{r,s=0}^{\infty} \mathbf{C}_n^r \mathbf{C}_m^s (-1)^{m-s} \\
 &\quad \times (C_A^\dagger)^r (C_B^\dagger)^s (D_A^\dagger)^{n-r} (D_B^\dagger)^{m-j}
 \end{aligned} \tag{15}$$

Where C^\dagger and D^\dagger are the operators on path C and path D in the same form of A^\dagger or B^\dagger according to their subscripts. \mathbf{C}_n^r is the number of different combinations of choosing r terms at a time from n terms.

Since we only consider the single photon state, we then trace off the subspace of path D and just retain the operators that produce single photon. Thus we derive the

single photon state ρ_H at the output port as:

$$\begin{aligned}
\rho_H &= e^{-(\alpha^2+3\beta^2)} \sum_{m+n=1}^{\infty} \left(\frac{1}{\sqrt{2^{m+n}} n! m!} \right)^2 \\
&\times [(\mathbf{C}_n^1 \sqrt{(n-1)!} \sqrt{m!})^2 \\
&\times (\alpha^2 + 3\beta^2)^{n-1} (2\beta^2)^m (\alpha^2 |H\rangle\langle H| + \beta^2 |V\rangle\langle V|) \\
&+ (\mathbf{C}_m^1 \sqrt{(m-1)!} \sqrt{n!})^2 \\
&\times (\alpha^2 + 3\beta^2)^n (2\beta^2)^{m-1} \beta^2 (|H\rangle\langle H| + |V\rangle\langle V|)] \\
&= e^{-(\alpha^2+3\beta^2)} \sum_{m+n=1}^{\infty} \frac{1}{2^{m+n}} \left[\frac{n}{n! m!} (\alpha^2 + 3\beta^2)^n (2\beta^2)^m \right. \\
&\times \left(\frac{\alpha^2}{\alpha^2+3\beta^2} |H\rangle\langle H| + \frac{\beta^2}{\alpha^2+3\beta^2} |V\rangle\langle V| \right) \\
&\left. + \frac{m}{m! n!} (\alpha^2 + 3\beta^2)^n (2\beta^2)^m \frac{1}{2} (|H\rangle\langle H| + |V\rangle\langle V|) \right] \\
&= e^{-(\alpha^2+3\beta^2)} \sum_{j=1}^{\infty} \left(\frac{1}{2} \right)^j \sum_{n=0}^j \\
&\times \left\{ \frac{n}{n!(j-n)!} (\alpha^2 + 3\beta^2)^n (2\beta^2)^{j-n} \right. \\
&\times \left[\frac{\alpha^2 - \beta^2}{\alpha^2 + 3\beta^2} |H\rangle\langle H| + \frac{2\beta^2}{\alpha^2 + 3\beta^2} \frac{1}{2} (|H\rangle\langle H| + |V\rangle\langle V|) \right] \\
&\left. + \frac{j-n}{n!(j-n)!} (\alpha^2 + 3\beta^2)^n (2\beta^2)^{j-n} \frac{1}{2} (|H\rangle\langle H| + |V\rangle\langle V|) \right\} \\
&\approx e^{-(\alpha^2+3\beta^2)} \sum_{j=1}^{\infty} \left(\frac{1}{2} \right)^j \frac{(\alpha^2+3\beta^2)^j}{(j-1)!} \left(\frac{\alpha^2 - \beta^2}{\alpha^2 + 3\beta^2} |H\rangle\langle H| \right) \\
&+ \sum_{j=1}^{\infty} \left(\frac{1}{2} \right)^j \frac{(j-1)(\alpha^2+3\beta^2)^{j-1} 2\beta^2}{(j-1)!} \left(\frac{\alpha^2 - \beta^2}{\alpha^2 + 3\beta^2} |H\rangle\langle H| \right) \\
&+ \sum_{j=1}^{\infty} \left(\frac{1}{2} \right)^j \frac{(\alpha^2+3\beta^2)^j}{(j-1)!} \frac{2\beta^2}{\alpha^2 + 3\beta^2} \frac{\hat{I}}{2} \\
&+ \sum_{j=1}^{\infty} \left(\frac{1}{2} \right)^j \frac{(\alpha^2+3\beta^2)^{j-1} 2\beta^2}{(j-1)!} \left[(j-1) \frac{2\beta^2}{\alpha^2 + 3\beta^2} \frac{\hat{I}}{2} + \frac{\hat{I}}{2} \right] \\
&\approx e^{-(\alpha^2+3\beta^2)} \\
&\times \sum_{j=0}^{\infty} \left(\frac{1}{2} \right)^{j+1} \frac{(\alpha^2+3\beta^2)^{j+1}}{j!} \\
&\times \left[\frac{\alpha^2 - \beta^2}{\alpha^2 + 3\beta^2} |H\rangle\langle H| + \frac{4\beta^2}{\alpha^2 + 3\beta^2} \frac{\hat{I}}{2} \right] \\
&= e^{-\frac{\alpha^2+3\beta^2}{2}} \left(\frac{\alpha^2+3\beta^2}{2} \right) \\
&\times \left(\frac{\alpha^2 - \beta^2}{\alpha^2 + 3\beta^2} |H\rangle\langle H| + \frac{4\beta^2}{\alpha^2 + 3\beta^2} \frac{\hat{I}}{2} \right) \\
&= N \cdot \left(\frac{r-1}{r+3} |H\rangle\langle H| + \frac{4}{r+3} \rho_{noise} \right).
\end{aligned}$$

(16) It is exactly Eq.(3) in the main text.

Where $\rho_{noise} \equiv \frac{1}{2} \hat{I} = \frac{|H\rangle\langle H| + |V\rangle\langle V|}{2}$, $N = e^{\frac{\alpha^2+3\beta^2}{2}} \cdot \frac{\alpha^2+3\beta^2}{2} \cdot \beta^2$ is the normalizing factor, and $r = \frac{\alpha^2}{\beta^2}$ equals to the definition of extinction ratio in Eq.(1). On the fourth step of this derivation, we make an approximation by neglecting the terms have coefficient $(2\beta^2)^i$ with order higher than 1, under the assumption of $\beta \ll \alpha$. Ignoring the normalizing factor, we can derive the single photon signal state as following:

$$\rho_{signal} = \frac{r-1}{r+3} \rho_{ideal} + \frac{4}{r+3} \rho_{noise}. \quad (17)$$

-
- [1] C. H. Bennet, G. Brassard, in *Processdings of the IEEE International Conference on Computers, Systems and Signal Processing, Bangalore, India (IEEE, New York)*, pp.175-179. (1984).
- [2] D. Mayers, *J.ACM* **48** 351 (2004).
- [3] P. W. Shor, J. Preskill, *Phys.Rev.Lett* **85** 441 (2000).
- [4] R. Renner, N. Gisin, B. Kraus, *Phys.Rev.A* **72** 012332 (2005).
- [5] R. Garca-Patrón, N. Cerf, *Phys.Rev.Lett* **97** 190503 (2006).
- [6] A. Leverrier, P. Grangier, *Phys.Rev.Lett* **102** 180504 (2009).
- [7] D. Gottesman, H.-K. Lo, N. Lütkenhaus, J. Preskill, *Quantum Inf. Comput.* **4** 325 (2004).
- [8] F. Grosshans, N. J. Cerf, *Phys.Rev.Lett* **92** 047905 (2004).
- [9] R. Garcia-Patrón, N. J. Cerf, *Phys.Rev.Lett* **97** 190503 (2006).
- [10] R. Renner, J. I. Cirac, *Phys.Rev.Lett* **102** 110504 (2009).
- [11] L. Lydersen et al., *Nat. Photonics* **4** 686 (2010).
- [12] V. Scarani, et al., *Rev.Mod.Phys* **81** 1301 (2009).
- [13] W.-Y. Hwang, *Phys. Rev. Lett.* **91** 057901 (2003).
- [14] X.-B. Wang, *Phys. Rev. Lett* **94** 230503 (2005).
- [15] H.-K. Lo, X. Ma, K. Chan, *Phys. Rev. Lett* **94** 230504 (2005).
- [16] X. Ma, B. Qi, Y. Zhao, H.-K. Lo, *Phys. Rev. A* **72** 012326 (2005).
- [17] H.-W. Li, et al., *Quant. Inf. Comp.* **10**, 771-779 (2010).
- [18] H.-W. Li, et al., *Quant. Inf. Comp.* **11**, 937-947 (2011).
- [19] T.-Y. Chen, et al., *Optics Express* **Vol.18** Issue 26, pp.27217-27225 (2010).
- [20] http://en.wikipedia.org/wiki/Extinction_ratio.
- [21] H.-K. Lo, J. Preskill, arXiv:quant-ph/0504209v1.
- [22] G. Brassard and L. Salvail, in *Advances in Cryptology*

EUROCRYPT '93, edited by T. Helleseth, Lecture Notes in Computer Science Vol. 765 (Springer, Berlin, 1994), pp. 410C423.

[23] S. Wang, et al., *Opt. Lett* **35** 14, 2454 (2010).